Introduction – Cryptography ≈ Crypto (암호기술, 암호)

Jong Hwan Park

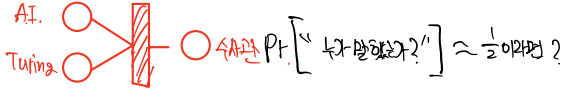
Class

- Cryptography
  - Lecture slides – eCampus every week

- Grading
  - Participation (10%)
  - Midterm exam (30%)
  - Final exam (30%)
  - Assignment (30%)

Cryptography in History (1)

- Classical cryptography
  - Caesar cipher
- World War II
  - Breaking Enigma (German) & Japan's cipher
  - ``The Imitation Game(2014)", "A Beautiful Mind(2001)"
- Claude Shannon (1949)
  - "Communication Theory of Secrecy Systems"
    - Information theory / entropy / perfect security of one-time pad / …
- John Nash and NSA (1955)
  - Suggest notion of modern cryptography 20 years ahead of time
  - Computational complexity (polynomial time vs. exponential time)
  - Suggest an encryption scheme (rejected)

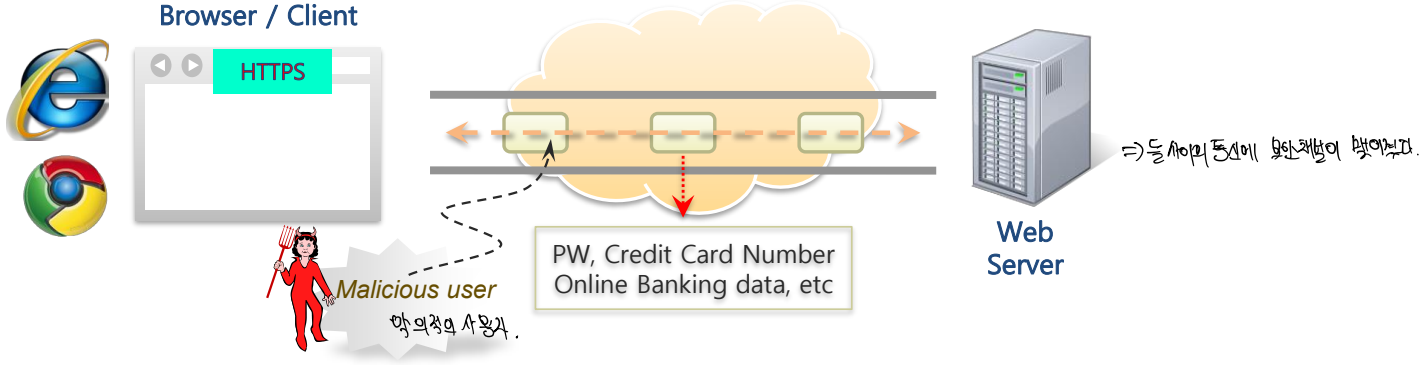


Cryptography in History (2)

- Diffie & Hellman (1976)
  - "New directions in cryptography" - pubic key cryptosystem
- Data Encryption Standard (DES) (1977)
  - Symmetric-key cipher
- RSA (1978)
  - Practical public key encryption scheme
- Recent crypto schemes (widely deployed)
  - AES / SHA-256 / RSA / (EC)-{DH, DSA} / …
- Post-Quantum Cryptography (PQC)
  - After 10~20 years, quantum algorithm will be used
  - Very recently, active researches are done for PQC

Recent Usage – Secure Channel (1)

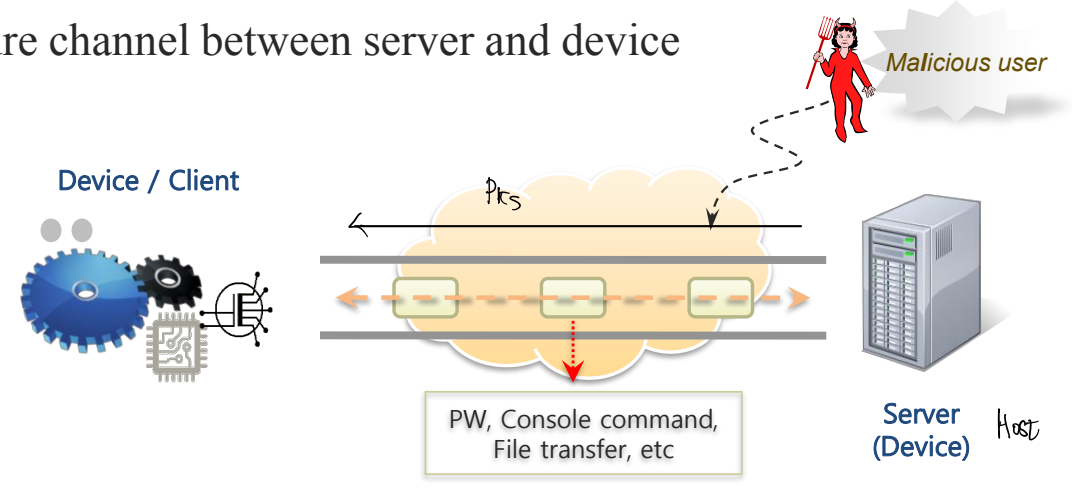
- SSL/TLS
  - Secure channel between web server and web browser



  - Server authentication using Cert(PK_S)
    => 서버 인증. = 인증서
  - User authentication (usually) over established secure channel
    => 사용자 인증.
  - Authenticated encryption protects real payload
  - Online banking, credit card payment, email protection,…

Recent Usage – Secure Channel (2)

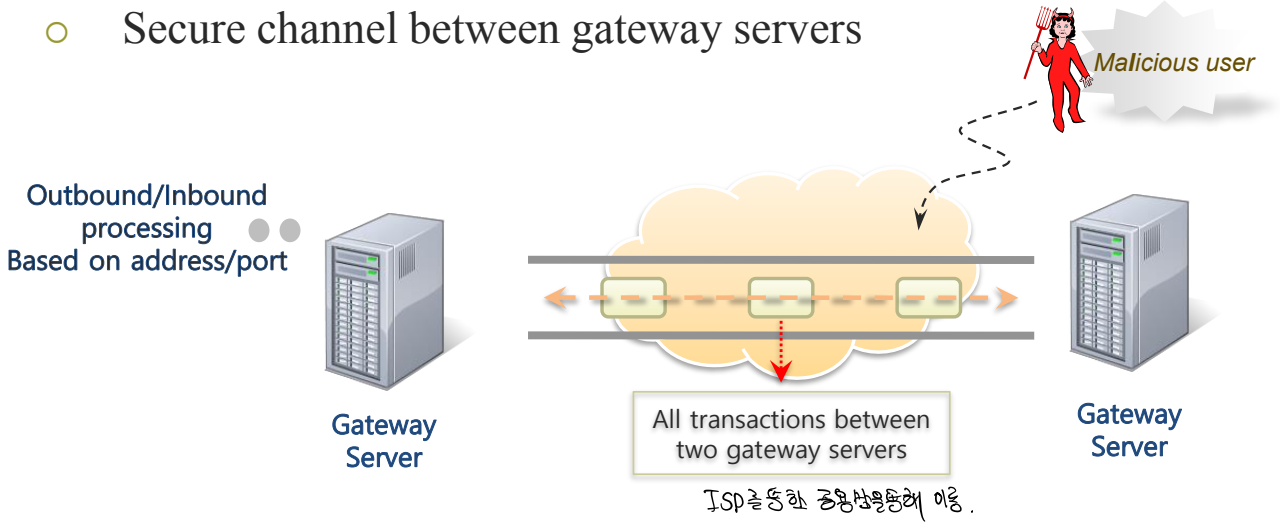
- SSH(Secure SHell)
  - Secure channel between server and device



  - Server authentication using raw host key (PK_S)
  - User authentication over established secure channel
  - Authenticated encryption protects real payload
  - Device(e.g., commercial board, server with Putty) access,…

Recent Usage – Secure Channel (3)

- IPSec IP level에서 암호화.
  - Secure channel between gateway servers



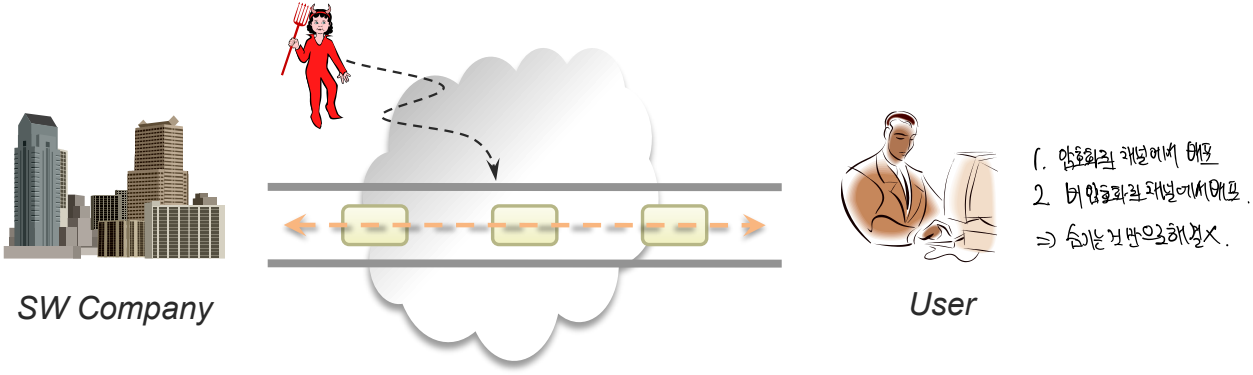
ISP를 통한 공용망을통해 이동.

  - Mutual authentication using {PSK, Cert(PK), PGP}
  - IKE(Internet Key Exchange) based on Diffie-Hellman
  - Authenticated encryption protects real payload
  - VPN, but too complex to set up IPSec,…

= 가장 사실망화
= IPSec의한 종류

Recent Usage – SW verification

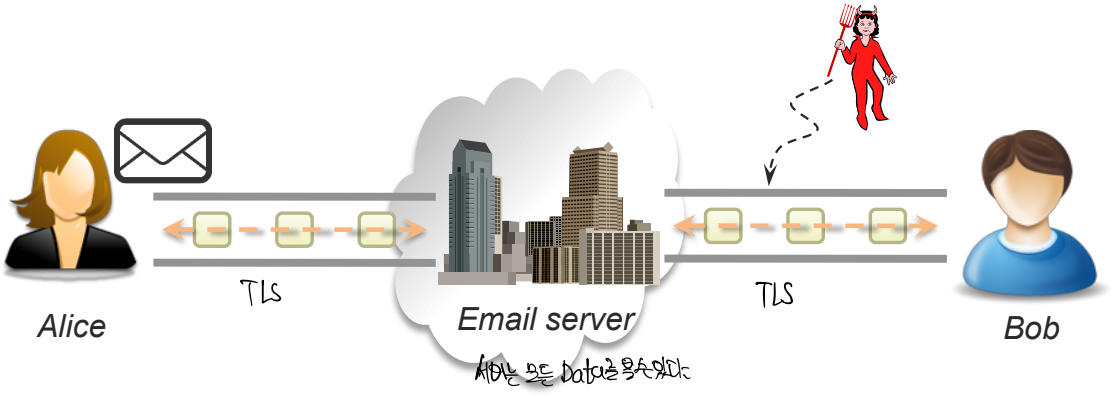
- Software distribution
  - A SW company wants to distribute a patch program to users



  - A malicious code can be injected into the patch
  - User needs to check if
    - (1) the patch comes from the authentic company and
    - (2) the patch is not changed during transmission
  - Integrity is required by using digital signature

Recent Usage – Email protection (1)

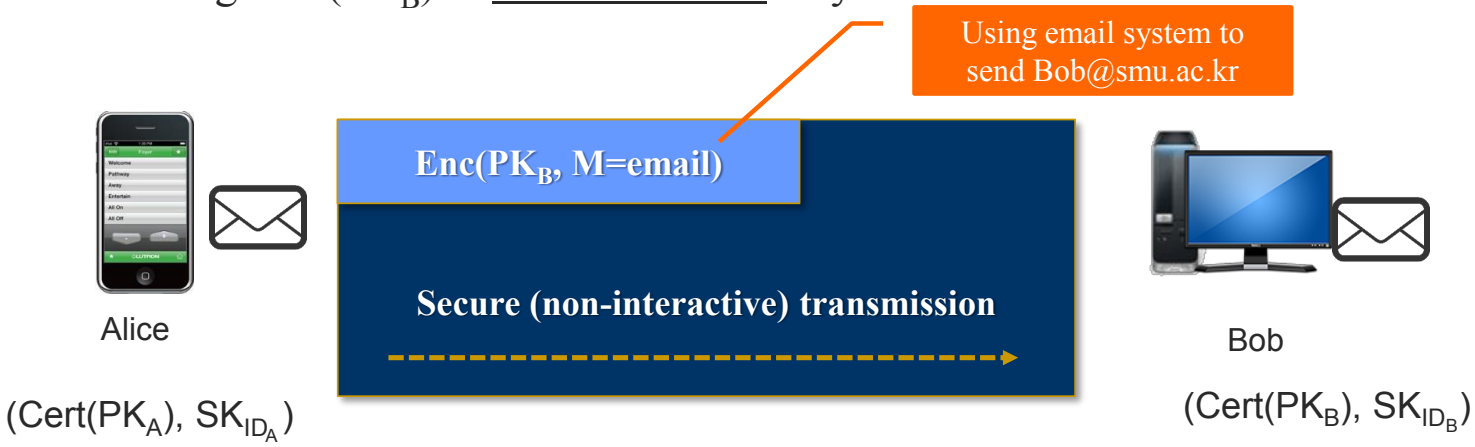
- Using email application with designated email server
  - E.g., {google, naver} mail



  - Problem: email server can see all contents of emails
  - This problem is the same as in other systems like the above
    - SNS(Social Network Services) like …

Recent Usage – Email protection (2)

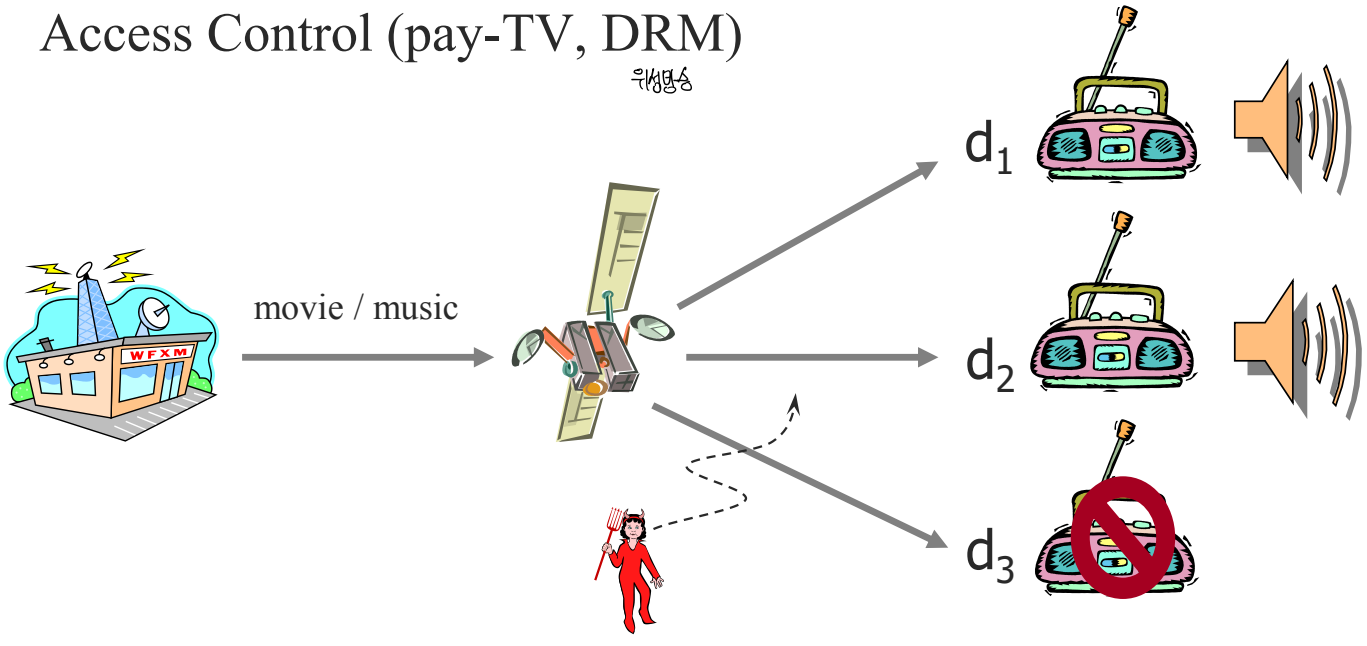
- End-to-end email protection
  - Using Cert(PK_B) in non-interactive way



  - Need to exchange (and manage) PK to each user
  - Recent solutions {PGP, S/MIME}, which are two complex to use

Recent Usage – Content protection

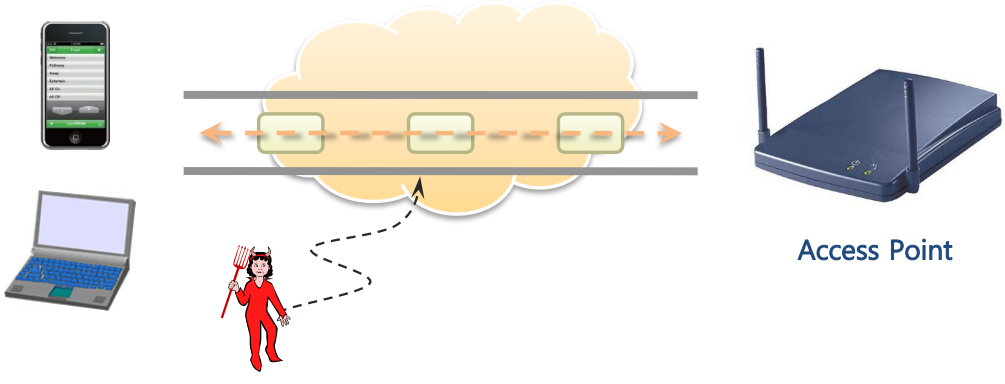
- Access Control (pay-TV, DRM)



  - Authorized users can have access to program (access control)
    - Revoked users should not have access to program
  - Keep program not available to non-authorized users (confidentiality)

Recent Usage – Access control

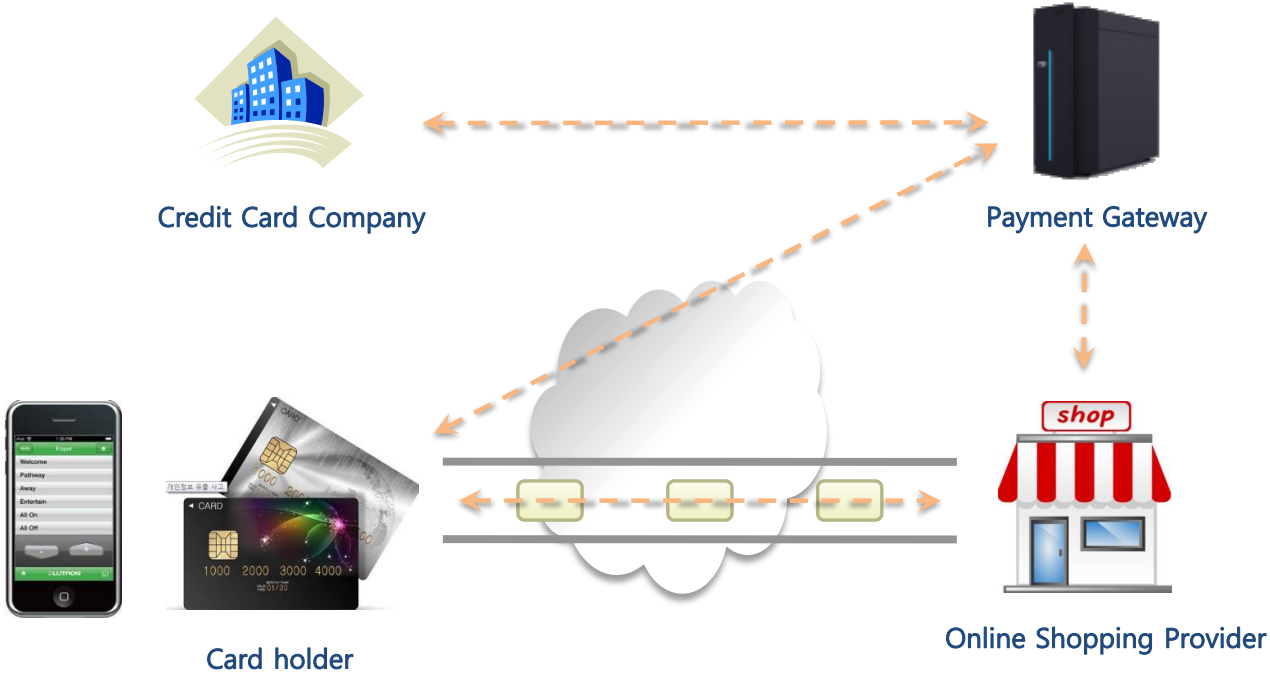
- IEEE 802.11 (wireless LAN security)



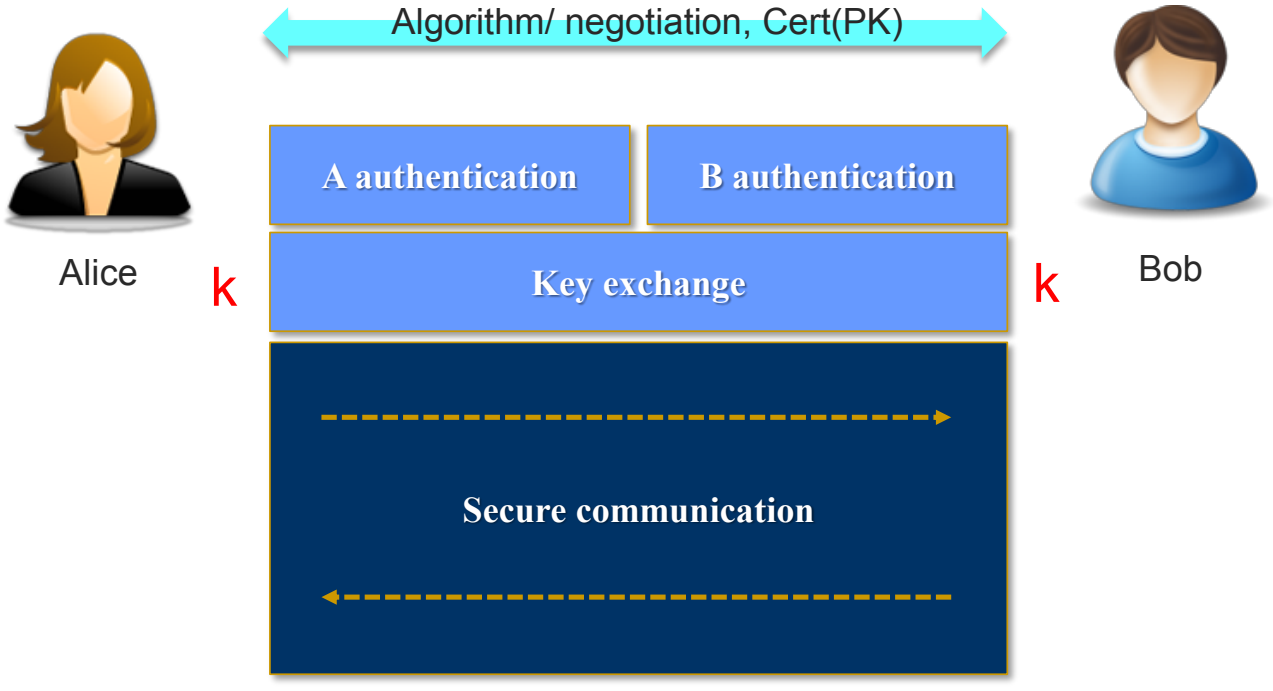
  - SSID/PW authentication (access control)
  - WEP/WAP/WAP2 are used for data protection
    - WEP has weakness

Recent Usage – Payment

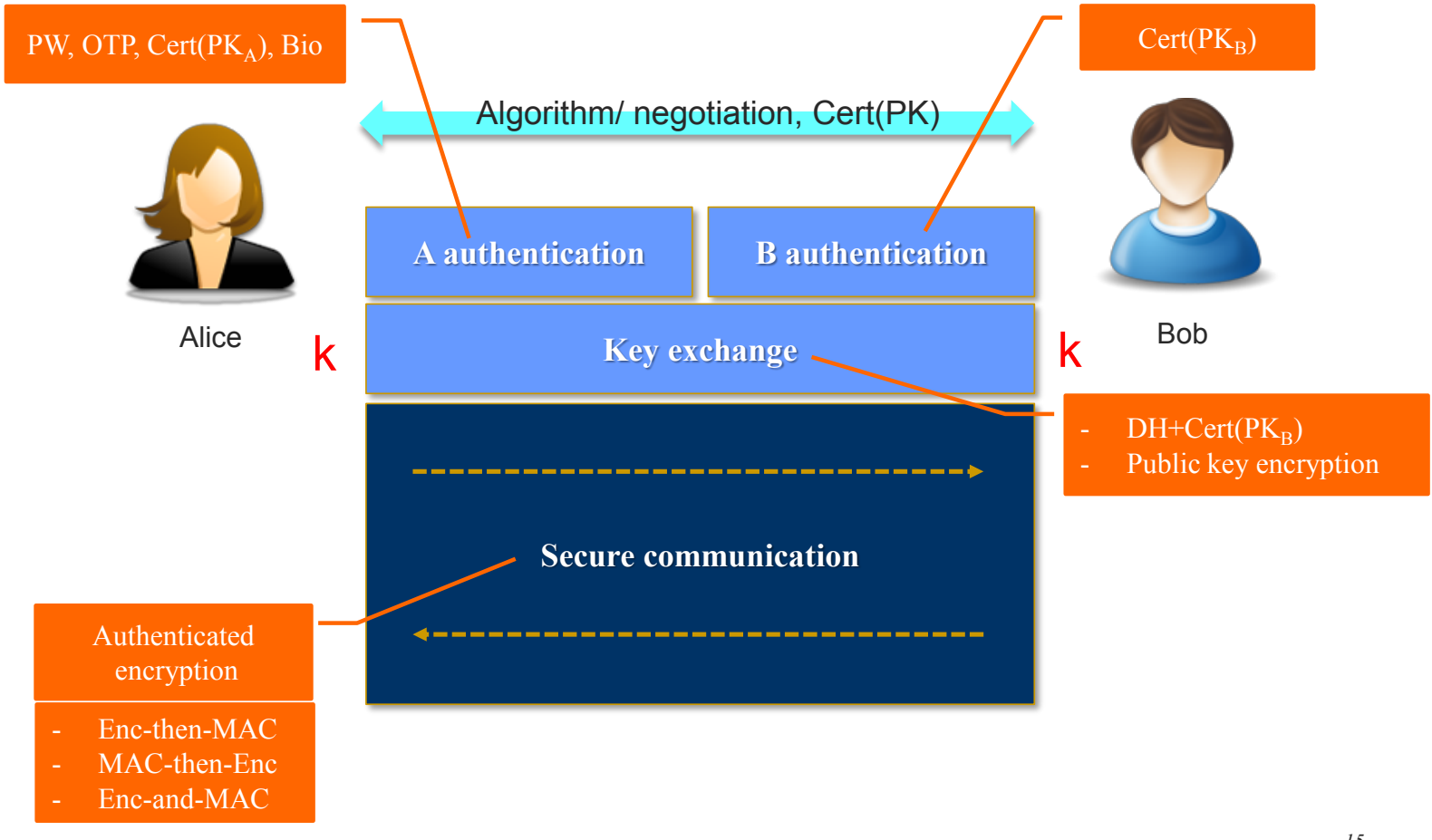
- Credit card payment
  - Simple payment methods
    - Amazon, PayPal / Samsung pay, Apple pay, Kakao pay, …



Crypto Core


Algorithm/ negotiation, Cert(PK)
A authentication
B authentication
Alice
k
Key exchange
k
Bob
Secure communication

Cryptographic Primitives



OS/System Security (beyond)

PW, OTP, Cert(PK_A), Bio

Cert(PK_B)

Algorithm/ negotiation, Cert(PK)

- TEE(Trusted Execution Environment)

Alice

A authentication

B authentication

Bob

Key exchange

- TEE(Trusted Execution Environment)

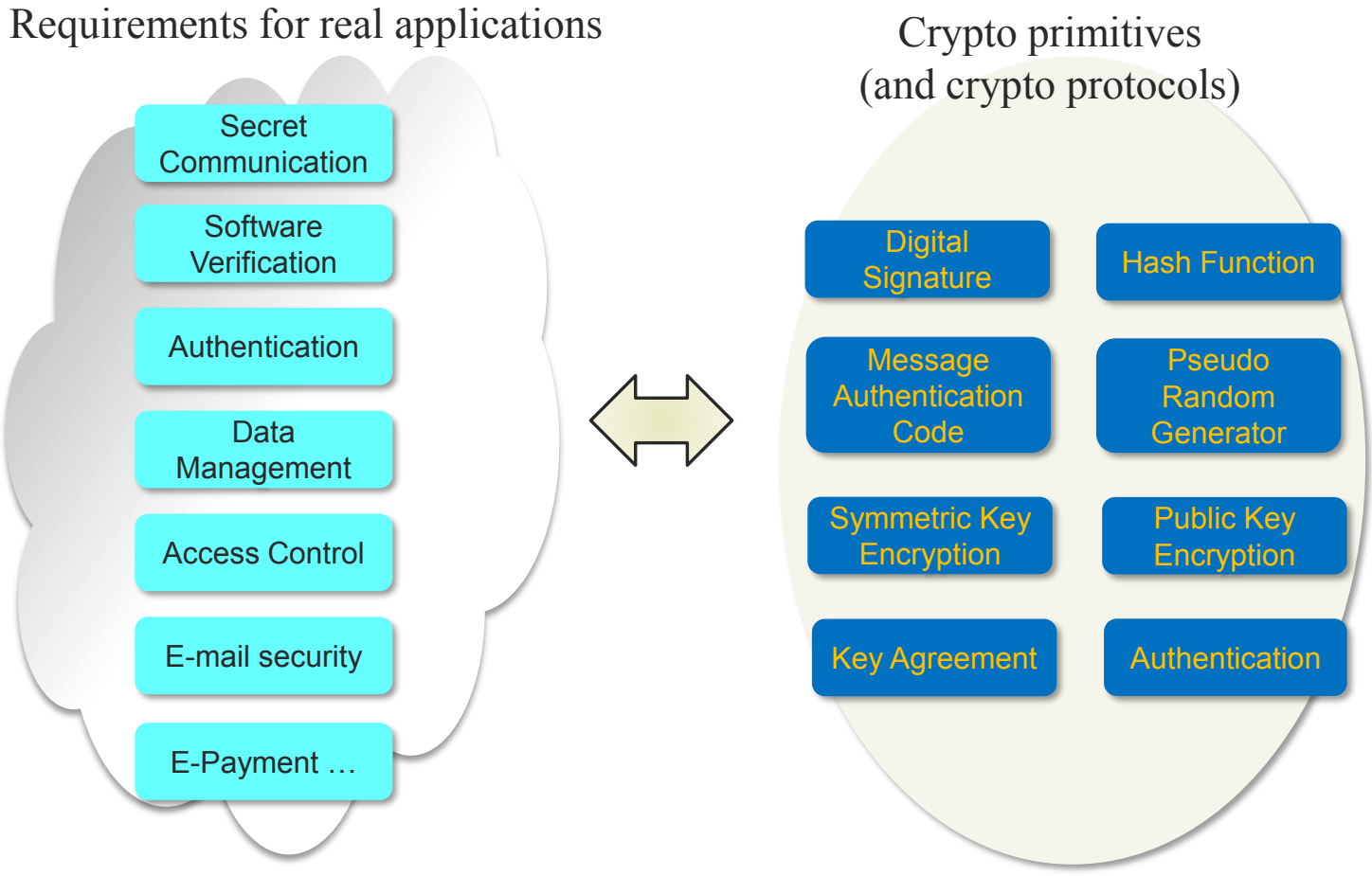
- DH+Cert(PK_B)
- Public key encryption

Secure communication

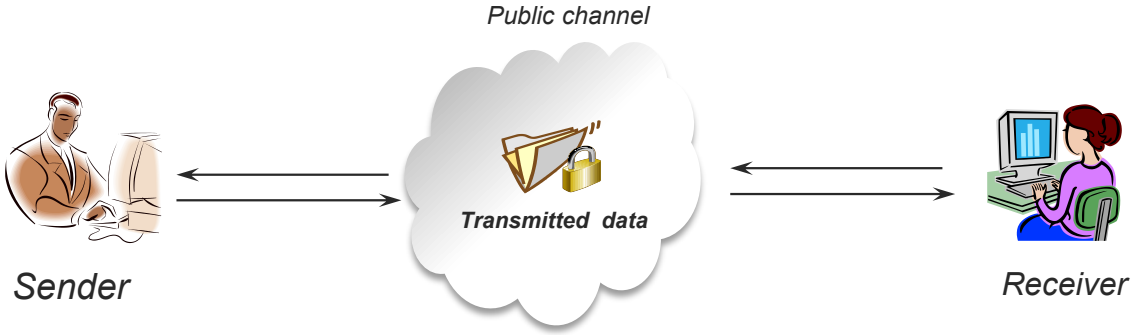
Authenticated encryption

- Enc-then-MAC
- MAC-then-Enc
- Enc-and-MAC

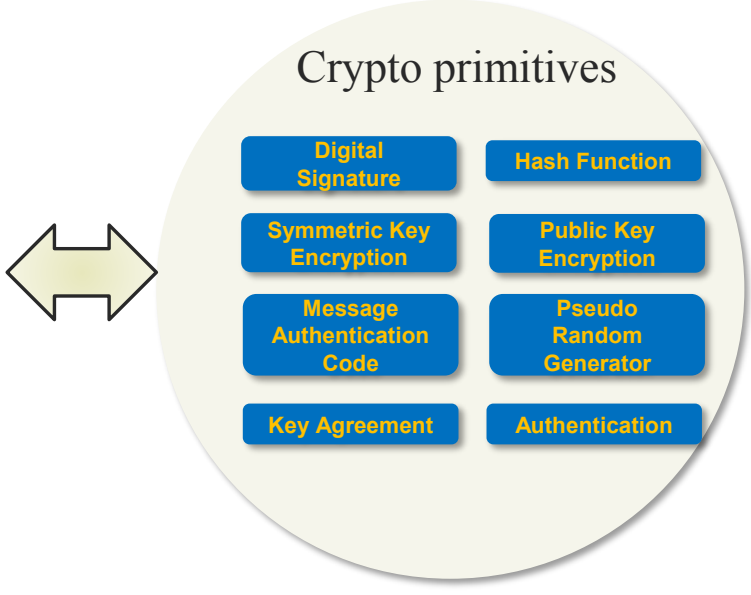
Requirements and Crypto primitives



Security Services



- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Access control (or availability)



Roadmap of the class

- In the class, we will go over
  - Basic primitives including
    - Symmetric-key encryption (via programming)
    - Hash function (via programming)
    - Message Authentication Code (via programming)
    - Public-key encryption
    - Digital signature
    - Authentication protocol (via programming)
    - Key agreement protocol
  - Some of crypto protocols like SSL/TLS, PGP, …